SENATE BILL No. 1279

Introduced by Senator Bowen

February 13, 2004

An act to add Sections 1785.11.25 and 1785.15.5 to, to add Title 1.81.21 (commencing with Section 1798.91) to Part 4 of Division 3 of, and to repeal and amend Sections 1798.29 and 1798.82 of, the Civil Code, relating to identity theft.

LEGISLATIVE COUNSEL'S DIGEST

SB 1279, as introduced, Bowen. Identity theft.

(1) Existing state and federal regulates the activities of consumer credit reporting agencies. Existing state law permits a consumer to put a security alert and a security freeze on the consumer's credit report, which act to notify a recipient of the credit report that the consumer's identity may been fraudulently used and to prohibit the release of the consumer's credit report without authorization, respectively.

This bill would require a consumer credit reporting agency to allow a consumer to add a password to the consumer's credit file, and would require that a prospective user of a consumer credit report match that password prior to releasing the consumer's credit report to the user. The bill would require that a consumer credit reporting agency provide a consumer a means of creating a password on the telephone and over the Internet, and as part of that process, the bill would require a consumer credit reporting agency to authenticate the identity of a consumer by requiring the consumer to provide specified information correctly. The bill would require a consumer reporting agency to permit a consumer to change a password, as specified, and would prohibit a consumer reporting agency from charging for any of these services. The bill would also require that a consumer reporting agency provide a toll-free telephone number staffed by people capable of answering and

appropriately responding to calls regarding a consumer's rights in connection with credit reports, 24 hours a day, each day of the year, as specified.

(2) Existing law requires any agency, or a person or business conducting business in California, which owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

This bill would expand the application of those provisions to all data, rather than only computerized data. The bill would require that an agency or a person or business that has suffered a breach of the security of the system to provide 2 years of a credit monitoring service, as defined, without charge to each person whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The bill would repeal duplicative provisions of law.

(3) Existing law protects the privacy of personal information by imposing various restrictions on the use of that information in a variety of commercial contexts. Existing law permits a business to swipe a driver's license or identification card only for specific purposes and prohibits a business from retaining information for purposes other than those specified.

This bill would prohibit a person or entity from storing specified personal information regarding a customer on a card key, which it would define as a card or other device that the person or entity uses to provide a customer access to a lodging or a facility or to goods or services associated with that lodging or facility.

Vote: majority. Appropriation: no. Fiscal committee: no. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 1785.11.25 is added to the Civil Code, immediately following Section 1785.11.2, to read:

1785.11.25. (a) A consumer credit reporting agency shall allow a consumer to add a password to the consumer's credit file. The consumer credit reporting agency shall require that a prospective user of a consumer credit report match that password

prior to releasing the consumer's credit report to the user. A consumer shall provide a prospective user of the consumer's credit report with the consumer's password as part of providing consent for the user to check the consumer's credit.

(b) (1) A consumer credit reporting agency shall provide a consumer a means of creating a password on the telephone and over the Internet.

(2) A consumer credit reporting agency shall authenticate the identity of a consumer who is creating a password by requiring the consumer creating the password to provide the following information correctly:

(A) The social security number, date of birth, name, and address of the consumer to whom the password will apply.

(B) The correct answer to at least two questions, based on information in the credit report of the consumer to whom the password will apply, that the consumer would be likely to know, but an identity thief would be unlikely to know.

(3) A consumer credit reporting agency shall require that the password be at least eight characters long and contain at least one letter and one number.

(c) A consumer shall be permitted to change his or her password by providing the existing password and following the process described in subdivision (b).

(d) A consumer credit reporting agency may not charge a fee for providing any of the services required by this section, including, but not limited to, creating or changing a password.

SEC. 2. Section 1785.15.5 is added to the Civil Code, to read:

1785.15.5. A consumer credit reporting agency shall provide consumers a toll-free telephone number that shall be staffed by people capable of answering and appropriately responding to calls related to a consumer's rights under this title, 24 hours a day, each day of the year. This telephone service shall be sufficiently staffed to provide that the average waiting period to speak with a live, customer service operator is not more than two minutes.

SEC. 3. Section 1798.29 of the Civil Code, as added by Chapter 915 of the Statutes of 2002, is repealed.

~~1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California~~

~~whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.~~

~~(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.~~

~~(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.~~

~~(d) For purposes of this section, ''breach of the security of the system'' means unauthorized aquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.~~

~~(e) For purposes of this section, ''personal information'' means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:~~

~~(1) Social security number.~~

~~(2) Driver's license number or California Identification Card number.~~

~~(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.~~

~~(f) For purposes of this section, ''personal information'' does not include publicly available information that is lawfully made~~

~~available to the general public from federal, state, or local government records.~~

~~(g) For purposes of this section, "notice" may be provided by one of the following methods:~~

~~(1) Written notice.~~

~~(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.~~

~~(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:~~

~~(A) E-mail notice when the agency has an e-mail address for the subject persons.~~

~~(B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.~~

~~(C) Notification to major statewide media.~~

~~(h) Notwithstanding subdivision (g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.~~

SEC. 4. Section 1798.29 of the Civil Code, as added by Chapter 1054 of the Statutes of 2002, is amended to read:

1798.29. (a) Any agency that owns or licenses ~~computerized~~ data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains ~~computerized~~ data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, ''breach of the security of the system'' means unauthorized acquisition of ~~computerized~~ data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, ''personal information'' means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section, ''personal information'' does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, ''notice'' may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(i) An agency that has suffered a breach of the security of the system shall provide two years of a credit monitoring service without charge to each person whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. For the purposes of this section, "credit monitoring service" means a service that allows a consumer electronic access to the information in his or her credit report on demand and provides regular e-mail notifications of changes to the consumer's credit report.

SEC. 5. Section 1798.82 of the Civil Code, as added by Chapter 915 of the Statutes of 2002, is repealed.

~~1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any~~

~~measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.~~

~~(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.~~

~~(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.~~

~~(d) For purposes of this section, ''breach of the security of the system'' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.~~

~~(e) For purposes of this section, ''personal information'' means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:~~

~~(1) Social security number.~~

~~(2) Driver's license number or California Identification Card number.~~

~~(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.~~

~~(f) For purposes of this section, ''personal information'' does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.~~

~~(g) For purposes of this section, ''notice'' may be provided by one of the following methods:~~

~~(1) Written notice.~~

~~(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.~~

~~(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:~~

~~(A) E-mail notice when the person or business has an e-mail address for the subject persons.~~

~~(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.~~

~~(C) Notification to major statewide media.~~

~~(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.~~

SEC. 6. Section 1798.82 of the Civil Code, as added by Chapter 1054 of the Statutes of 2002, is amended to read:

1798.82. (a) Any person or business that conducts business in California, and that owns or licenses ~~computerized~~ data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains ~~computerized~~ data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery,

if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, ''breach of the security of the system'' means unauthorized acquisition of ~~computerized~~ data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, ''personal information'' means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section, ''personal information'' does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, ''notice'' may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject

persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the person or business has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(i) A person or business that has suffered a breach of the security of the system shall provide two years of a credit monitoring service without charge to each person whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. For the purposes of this section, "credit monitoring service" means a service that allows a consumer electronic access to the information in his or her credit report on demand and provides regular e-mail notifications of changes to the consumer's credit report.

SEC. 7. Title 1.81.21 (commencing with Section 1798.91) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.81.21. CARD KEYS

1798.91. (a) For the purposes of this section, ''card key'' means a card or other device that a person or entity uses to provide a customer access to a lodging or a facility or to goods or services associated with that lodging or facility.

(b) A person or entity may not store the following personal information of a customer on a card key:

(1) Name.

(2) Address.

(3) Telephone number.

(4) Birth date.

(5) Social security number.
(6) Driver's license number.
(7) Credit card number.
(8) Bank account number.

O